3. How can you install Nessus on various operating systems?

📌 How to Install Nessus on Various Operating Systems

Nessus, developed by **Tenable**, is a powerful **vulnerability scanner** used for identifying security weaknesses in networks, applications, and systems. Below are the steps to install Nessus on **Linux, Windows, and macOS**.

🔹 1. Install Nessus on Linux (Debian-based & RHEL-based)

Nessus supports **Debian-based (Ubuntu, Kali) and RHEL-based (CentOS, Fedora, Rocky Linux)** distributions.

🛠️ Step 1: Download Nessus Package

Visit the official Tenable download page:
🔗 https://www.tenable.com/downloads/nessus

Choose the appropriate package:

- **Debian-based (Ubuntu/Kali):** `.deb` package
- **RHEL-based (CentOS/Rocky):** `.rpm` package

Alternatively, you can use `wget` to download directly:

```
# Debian-based (Ubuntu/Kali)
wget https://downloads.tenable.com/nessus/nessus_latest_amd64.deb

# RHEL-based (CentOS/Rocky/Fedora)
wget https://downloads.tenable.com/nessus/nessus_latest_x86_64.rpm
```

🛠️ Step 2: Install Nessus

✅ For Debian-based (Ubuntu/Kali):

```
sudo dpkg -i nessus_latest_amd64.deb
```

✅ For RHEL-based (CentOS/Rocky):

```
sudo rpm -ivh nessus_latest_x86_64.rpm
```

🛠️ Step 3: Start Nessus Service

Once installed, enable and start the Nessus service:

```
sudo systemctl enable nessusd
sudo systemctl start nessusd
```

Check if Nessus is running:

```
sudo systemctl status nessusd
```

🛠 Step 4: Access Nessus Web Interface

Nessus runs on **port 8834**. Open a web browser and navigate to:

```
https://localhost:8834
```

You will see the Nessus setup page.

🔹 2. Install Nessus on Windows

🛠 Step 1: Download Nessus Installer

Go to the official Nessus download page:
🔗 https://www.tenable.com/downloads/nessus

Download the **Windows (.exe) installer**.

🛠 Step 2: Install Nessus

1. Run the downloaded `.exe` file.
2. Follow the **on-screen installation instructions**.
3. When prompted, choose **Nessus Essentials (Free), Nessus Professional, or Nessus Expert**.

🛠 Step 3: Start Nessus Service

After installation, Nessus runs as a **Windows service**. To verify:

1. Press `Win + R`, type `services.msc`, and hit **Enter**.
2. Look for **Tenable Nessus** and ensure it's **running**.

🛠 Step 4: Access Nessus Web Interface

Open a browser and go to:

```
https://localhost:8834
```

Complete the setup and create an account.

🔹 3. Install Nessus on macOS

🛠️ Step 1: Download Nessus for macOS

Download the **macOS (.dmg) installer** from:
🔗 https://www.tenable.com/downloads/nessus

🛠️ Step 2: Install Nessus

1. Open the **.dmg** file and drag the Nessus application to the **Applications folder**.
2. Follow the **on-screen installation process**.

🛠️ Step 3: Start Nessus Service

To start Nessus manually, open **Terminal** and run:

```
sudo launchctl load /Library/LaunchDaemons/com.tenable.nessus.plist
```

To check if Nessus is running:

```
sudo launchctl list | grep nessus
```

🛠️ Step 4: Access Nessus Web Interface

Once installed, open:

```
https://localhost:8834
```

Complete the setup process and **activate Nessus**.

🔹 4. Nessus Activation & Setup

During the initial setup, you must **activate Nessus**. Choose one of the following editions:

- **Nessus Essentials (Free)** – For personal and learning use.
- **Nessus Professional** – Paid version for enterprise security.
- **Nessus Expert** – Advanced security scanning with more features.

To activate:

1. Enter your **activation code** from **Tenable**.
2. Nessus will **download and install plugins** (this may take a few minutes).
3. After setup, start scanning your systems! 🚀

🔹 5. Verify Nessus Installation

To ensure Nessus is working, check:

✅ **Service Status:**

```
# Linux
sudo systemctl status nessusd

# macOS
sudo launchctl list | grep nessus
```

✅ **Web Interface:**
Go to `https://localhost:8834` in your browser.

🎯 Final Notes

✓ **Nessus is a crucial tool for vulnerability assessment** in **penetration testing, bug bounty, and cybersecurity defense**.
✓ Make sure to **update Nessus plugins** regularly for accurate vulnerability detection.
✓ Run **authenticated scans** for deeper security insights.